# Appendix X - Safety case analysis

September 6, 2022

## 0.1 Introduction

AdvoCATE is a safety case tool for UAVs created by NASA. It is a peer reviewed tool which can map the operation hazards and help the user employ suiting mitigations[1, 2, 3, 4, 5]. In this appendix, the tool has been used to perform an analysis of the HealthDrone 3.0 safety architecture to show compliance with the SAIL IV technical requirements of OSO #05, #10 & #12, #19 and SORA Step #9.

## 0.2 Functional Hazard Analysis

Before using AdvoCATE, a Functional Hazard Analysis (FHA) is performed. The high level UAS functions have been identified, as well as their failure conditions, breakdown of failure conditions, failure effects and classification of effects[6]. The results are shown in table 1.

| **Function** | **Failure condition** | **Breakdown of failure condition** | **Effect of failure condition** | **Classification of effect** |
|---|---|---|---|---|
| Control altitude | Inability to control altitude | Propulsion failure | Crash into ground | Catastrophic |
| | | Power failure | | |
| | | FC failure | | |
| Control lateral position | Inability to control lateral position | Propulsion failure | Exit flight geography | Hazardeous |
| | | FC failure | | |
| C2 link communication | Inability to communicate C2 | UAV radio failure | Pilot removed from loop (BVLOS) | Major |
| | | GCS radio failure | | |
| Provide HMI | Inability to provide HMI for GCS | HMI failure | Pilot removed from loop (BVLOS) | Hazardeous |
| TX remote control | Inability to remote control UAV | TX failure | Pilot partially removed from loop | Major |
| Perform DAA | Inability to perform DAA | DAA failure | Loss of air separation | Hazardeous |

Table 1: Table of functions and their failures. This table has been used as input in AdvoCATE.

## 0.3 AdvoCATE explainer

The AdvoCATE process consists of the following four steps: system decompositions and hazard identification, risk analysis, risk assessment, and risk mitigation.

The first step is *system decompositions and hazard identification* which starts by splitting the UAS into its physical submodules and annotating these in the AdvoCATE Domain Specific Language (DSL). Then a Functional Hazard Assessment (FHA) is performed and the identified failure-capable functions are also annotated in the AdvoCATE DSL. Based on the physical and functional decompositions written in the DSL, the functional failures and their physical causes are linked and their consequences written down. E.g. loss of propulsion will have the consequence "crash into ground". During the *risk analysis* step, the consequences are given failure classifications, taken from the FHA, such as minor or catastrophic. Each failure component is given a quantifiable probability, which enables AdvoCATE to calculate the combined probability of a consequence with multiple possible failure components. AdvoCATE then generates Bow-Tie Diagrams (BTDs), which is a visual representation of the above-mentioned data. Step three is *risk assessment*, in which the BTDs are examined. An example is shown in figure 1.

From the EASA Special Condition, titled Equipment, systems, and installations[8], we find a requirement table linking severities and their maximum allowed probabilities. This table is shown in figure 2.

By looking at figure 1 we see that it is currently Remote, which is too high a probability.

This leads to the final step *risk mitigation* where all consequences with a RL too high for their RS are noted. Then, mitigations are instated to bring the likelihood down to an acceptable value. The mitigations can be instated either to reduce the likelihood of the individual failure component (blue boxes in figure 1) or they can be instated after the functional failure (orange circle) has happened, to avoid the consequence (red box) taking place. Staying with the example from figure 1, we insert a mitigation after altitude control has been lost, as seen in figure 3.

As the consequence is now extremely improbable, the requirements from EASAs "Equipment, systems, and installations", shown in figure 2 are now complied with. This is repeated for all functional failures, until all complies.

## 0.4 Safety case analysis results

In this section, the safety case analysis results will be presented. Table 2 shows an overview of the events, or functional failures, their possible causes (threats), the consequences and finally the severity and initial likelihood, the barriers instated and the resulting likelihoods. This is shown for take-off. For Cruise, the RTL barrier is removed. Compared with the table in figure 2, we see that all risks are sufficiently mitigated.

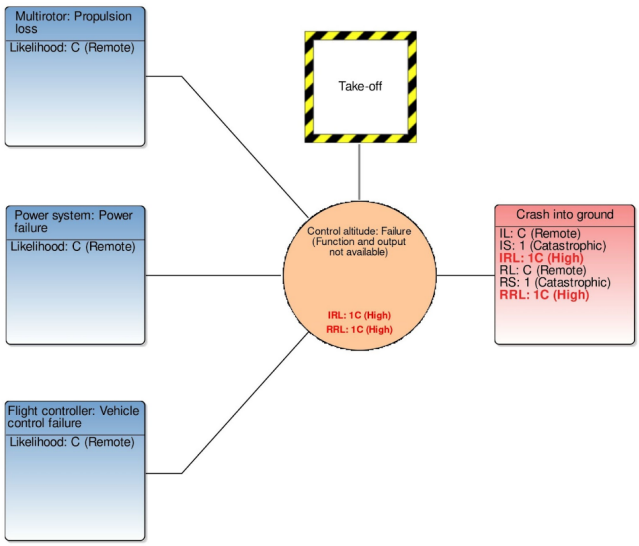


Figure 1: A BTD structure generated by AdvoCATE for the failure to control altitude. This can have the causes, or threats in AdvoCATE, shown to the left such as propulsion loss. We can also see that this specific BTD is for failure to control altitude during take-off. Finally, the red box shows the consequence of this failure, which is crash into ground. The Initial Likelihood (IL) is Remote, while the Initial Severity (IS) is Catastrophic. The Resulting Likelihood (RL) and Resulting Severity (RS) are equal to the IL and IS, as no mitigations has been instated.

| **Classification of Failure Conditions (Note 4)** | | | | |
|---|---|---|---|---|
| No Safety Effect | Minor | Major | Hazardous | Catastrophic |
| **Allowable Qualitative Probability (Note 4)** | | | | |
| No Probability Requirement | Probable | Remote | Extremely Remote | Extremely Improbable |
| **Allowable Quantitative Probabilities (Note 2) (Note 4)** | | | | |
| No Probability Requirement | $<10^{-3}$ (Note 1) | $<10^{-4}$ (Note 1) | $<10^{-6}$ | $<10^{-8}$ (Note 3) |

Figure 2: This table shows that for a catastrophic failure, the probability must be extremely improbable[8]

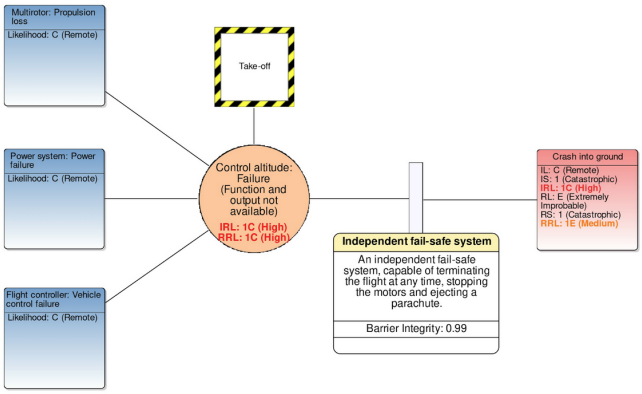


Figure 3: The same BTD structure as in figure 1, only now a mitigation has been inserted. The chosen mitigation is a failsafe system with a parachute, which reduces ground impact. The fail-safe system has been thoroughly tested and thus has a barrier integrity of 0.99. The consequence box now shows that the RL is Extremely Improbable.

### 0.4.1 Bow-Tie Diagrams

In the following, the BTDs are shown. Take-off and landing BTDs are virtually the same, as both happens in VLOS conditions for these operations. Thus, only take-off is shown.

#### Take-off and landing

Figures: 4, 5, 6, 7, 8, 9.

| Event | Threat(s) | Consequence | S | IL | Barrier(s) | RL |
|---|---|---|---|---|---|---|
| Failure to control altitude | - Control failure<br>- Power failure<br>- Propulsion loss | TO/L: Crash into ground | C | R | IFS | EI |
| | | Cr: Crash into ground | C | R | IFS | EI |
| Failure to control lateral position | - Navigation failure<br>- Propulsion loss | TO/L: Deviation from flight path | H | R | RTL, IFS | EI |
| | | Cr: Deviation from flight path | H | R | IFS | EI |
| C2 link failure | - GCS C2 failure<br>- UAV C2 failure | TO/L: Control reduced to manual | M | P | RTL, IFS | EI |
| | | Cr: Pilot removed from loop | H | P | IFS | ER |
| HMI failure | - Computer failure | TO/L: Control reduced to manual | M | P | RTL, IFS | EI |
| | | Cr: Pilot removed from loop | H | P | IFS | EI |
| TX failure | - Battery failure<br>- Hardware failure | TO/L: Control reduced to C2 | M | P | RTL, IFS | EI |
| | | Cr: Not detectable and no impact | - | - | - | - |
| DAA failure | - System failure | TO/L: Possible loss of separation with GA | H | P | RTL, IFS | EI |
| | | Cr: Possible loss of separation with GA | H | P | IFS | ER |

Table 2: Abbreviations used: **T**ake-**O**ff, **C**ruise, **L**and, **S**everity, **M**ajor, **H**azardous, **C**atastrophic, **I**nitial **L**ikelihood, **R**esidual **L**ikelihood, **R**emote, **E**xtremely **R**emote, **E**xtremely **I**mprobable, **I**ndependent **F**ailsafe **S**ystem, **R**eturn **T**o **L**and. For some events, the consequence and/or mitigations vary depending on the system state. For instance, losing C2 communication is less severe during take-off and landing, as the remote pilot will be able to take manual control and land the UAV.

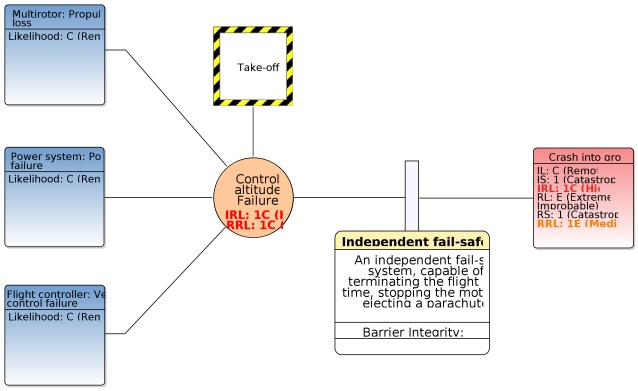


Figure 4: Failure to control altitude.

**Cruise**

Figures: 10, 11, 12, 13, 14.

## 0.5 Safety case conclusion

The tables and figures above present the analysis results. Based on these, we conclude that the potential risks are sufficiently mitigated, using the independent failsafe system.

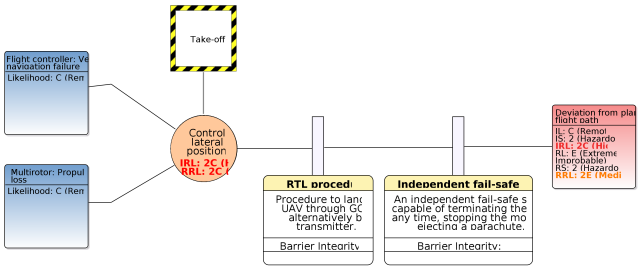


Figure 5: Failure to control lateral position.

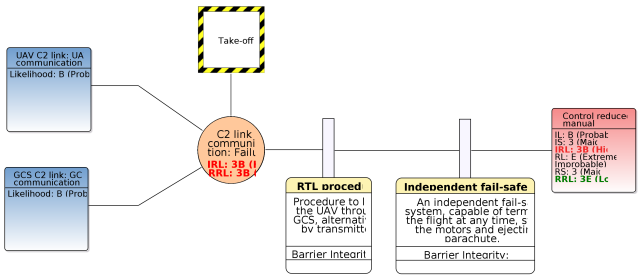


Figure 6: Failure to communicate via C2.

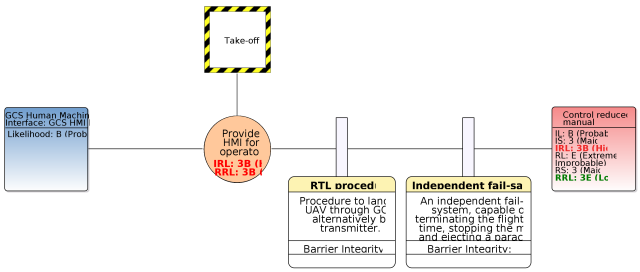


Figure 7: Failure to produce Human Machine Interface.

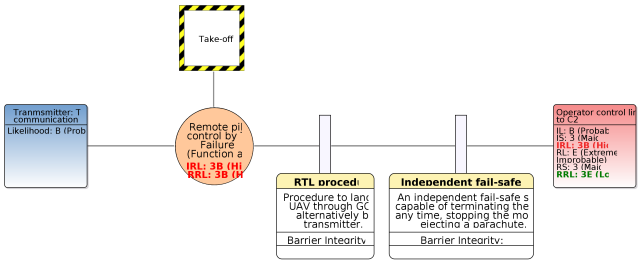


Figure 8: Failure to control via TX.

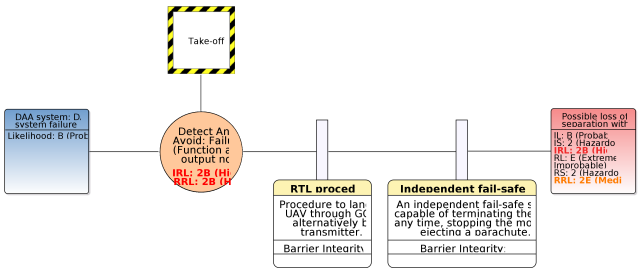


Figure 9: Failure to perform Detect And Avoid.

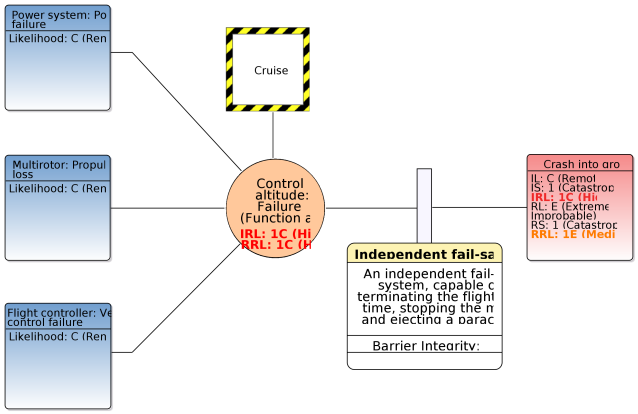


Figure 10: Failure to control altitude.

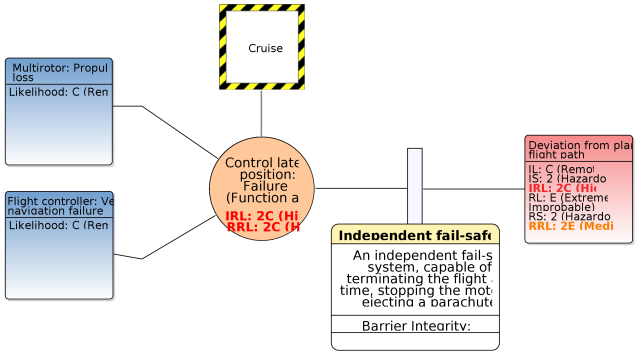


Figure 11: Failure to control lateral position.

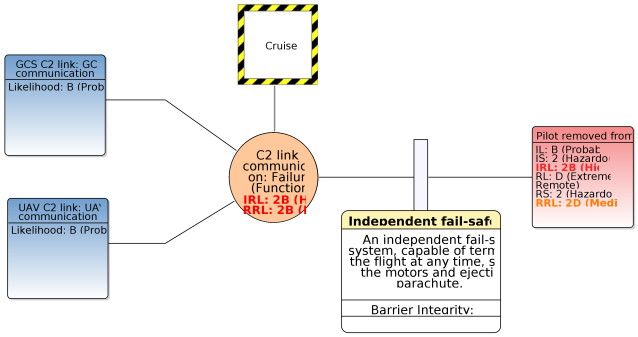


Figure 12: Failure to communicate via C2.

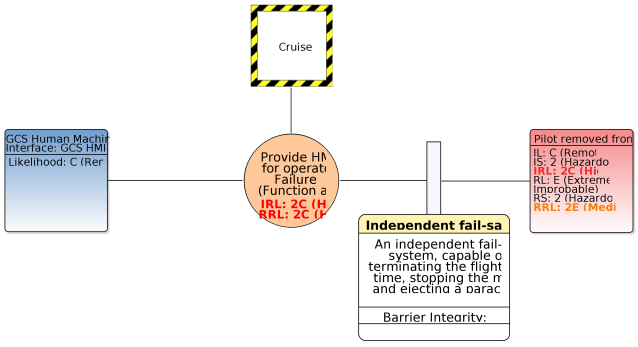


Figure 13: Failure to produce Human Machine Interface.

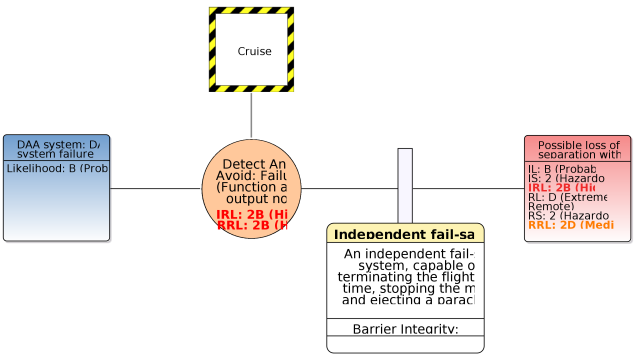


Figure 14: Failure to perform Detect And Avoid.

# Bibliography


[1] Denney, E., Pai, G., & Whiteside, I. (2017, September). Modeling the safety architecture of UAS flight operations. In International Conference on Computer Safety, Reliability, and Security (pp. 162-178). Springer, Cham.

[2] Clothier, R., Denney, E., & Pai, G. J. (2017). Making a risk informed safety case for small unmanned aircraft system operations. In 17th AIAA Aviation Technology, Integration, and Operations Conference (p. 3275).

[3] Denney, E., Pai, G., & Johnson, M. (2018, September). Towards a rigorous basis for specific operations risk assessment of UAS. In 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC) (pp. 1-10). IEEE.

[4] Denney, E., Pai, G., & Whiteside, I. (2017, September). Model-driven development of safety architectures. In 2017 ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS) (pp. 156-166). IEEE.

[5] Denney, E., & Pai, G. (2015, August). A methodology for the development of assurance arguments for unmanned aircraft systems. In 33rd International System Safety Conference (ISSC 2015).

[6] Sae International. (1996). Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment (ARP4761). SAE International.

[7] Laursen, K. H & Jensen, K. (2022). Achieving Technical SORA SAIL IV Compliance.

[8] European Union Aviation Safety Agency (2015). Special Condition for Equipment, systems, and installations, SC-RPAS.1309-01.